CLAIM(S):

1.   A system for anonymous Internet transactions, the system comprising:

a web portal, the web portal having a connection with the Internet;

a plurality of web servers for hosting transactions between users, each web server in network communication with the web portal;

a plurality of data stores for storing the transactions wherein a data store is associated with each web server; and

a privacy agent for programmatically maintaining transactional anonymity between users on the web servers.

2.   The system of claim 1, wherein the privacy agent comprises:

a software component stored on a computer, the software agent being in network communication with each web server, the software agent programmatically monitoring text messages between the web portal and the web servers.

3.   The system of claim 2, wherein the privacy agent further comprises:

privacy rules for identifying private data within the text messages, the privacy agent programmatically interfering with text messages that contain the private data according to the privacy rules.

4.   The system of claim 3, wherein programmatically interfering with text messages includes temporarily preventing a message from reaching the web servers until a sender of the message authorizes disclosure of the private data.

5.   The system of claim 1, wherein the plurality of data stores comprise:

a plurality of databases for storing records associated with users on the web server, each database being associated with one of the plurality of data stores.

6.   The system of claim 5, wherein the records contain information about users, each record having information about one user, the information comprising:

an actual identity of the one user, the actual identity of the one user being validated by a credit card transaction;

privacy preferences associated with the one user, the privacy preferences for controlling revelation of the actual identity of the one user;

messages generated by the one user; and

a preferred contact method for the one user, the preferred contact method being used by the system to automatically send notices to each user.

7.   The system of claim 6, wherein the actual identity comprises a name, a mailing address, city, state, e-mail address, and telephone numbers, wherein the privacy preferences permit the one user to gradually reveal the actual identity to another user such that the one user may reveal the name to another user without disclosing other information.

8.   A method for protecting users from inadvertent disclosure of identifying information on a computer bulletin board, the method comprising:

monitoring text message transmissions programmatically using a privacy agent, the privacy agent residing on a computer network with a web server that hosts the computer bulletin board;

scanning the text message for identifying information; and

interfering temporarily with transmission of the text message if the text message contains identifying information regarding an actual identity of a sender of the text message.

9.   The method of claim 8, wherein interfering temporarily with transmission comprises:

warning the sender that the .text message contains identifying information;

prompting the sender to authorize disclosure of the identifying information;

processing the text message by posting the text message to the web server if the sender authorizes the disclosure or rejecting the text message if the sender fails to authorize the disclosure.

10.   The method of claim 8, and further comprising:

posting the text message to a private area on the web server;

notifying an intended recipient that the text message has been posted.

11.   The method of claim 10, wherein notifying an intended recipient comprises:

determining programmatically to whom the sender intends to send the text message;

retrieving a preferred contact method for the intended recipient, the preferred contact method specifying a means for contacting the intended recipient; and

notifying the intended recipient of the text message programmatically using the preferred contact method.

12. A method for allowing anonymous Internet negotiations, the method comprising:

prompting a user on a web server to establish an account on the web server;

validating an actual identity of the user before registering the user and creating the account on the web server;

allowing the registered user to submit transactional information to the web site;

monitoring the transactional information programmatically using a privacy agent; and

interfering temporarily with transmission of the transactional information if the privacy agent detects information corresponding to the actual identity of the registered user.

13. The method of claim 12, and further comprising:

transmitting the transactional information to the web server for storing in a data store; and

providing marketing opportunities to the registered user, the marketing opportunities including stickers, flyers, and e-mail to other registered users.

14. The method of claim 13, wherein providing marketing opportunities comprises:

offering the registered user a choice of marketing opportunities;

offering the registered user an option of marketing the transactional information or of having the system distribute marketing materials to attract Internet users to the transactional information; and

processing the choice and the option by preparing marketing materials and mailing the marketing materials to the registered user, and if the registered user chooses, displaying marketing materials on behalf of the registered user.

15.   The method of claim 12, and further comprising;

permitting a second user to view the transactional information over the Internet;

requiring the second user to establish an account on the web server before permitting the second user to respond to the transactional information, the second user being required to enter information including a credit card number to establish an account, the information including an actual identity of the second user;

validating the actual identity of the second user according to the credit card number;

permitting the second user to post a response, the response being associated with the transactional information;

monitoring the response programmatically using a privacy agent; and

interfering temporarily with transmission of the response if the privacy agent detects information corresponding to the actual identity of the second user.

16.   The method of claim 15, wherein interfering temporarily with the transmission of the response comprises:

scanning the response for text corresponding to the actual identity of the second user; and

processing the response by posting the response to the web server if no text corresponding to the actual identity of the second user is found or requiring the second user to authorize disclosure of the text corresponding to the actual identity of the second user.

17.   The method of claim 12, wherein monitoring the transactional information programmatically comprises:

scanning text of the transactional information for phone numbers, addresses, names, e-mail addresses, and cities corresponding to the actual identity of the user.

18.   The method of claim 15, wherein monitoring the transactional information programmatically comprises:

scanning text of the response for phone numbers, addresses, names, e-mail addresses, and cities corresponding to the actual identity of the second user.

19.   The method of claim 12, and further comprising:

generating automatically a pin number for the user, the pin number serving as a pseudonym for the user on the web server.

20.   The method of claim 15, and further comprising:

generating automatically a pin number for the second user, the pin number serving as a pseudonym for the second user on the web server.